CHAPTER

1

INTRODUCTION TO ACTIVE DIRECTORY

After completing this chapter, you will be able to:

- Discuss the main goals Microsoft set for Windows 2000 development
- Describe the different versions of Windows 2000
- Describe the main purpose for each version for Windows 2000
- Describe and define some of the key new features that have been introduced in Windows 2000
- Define and describe the goal and purpose of a directory service
- Describe the ways in which networks have used directory services in the past
- Describe the main areas of improvement for system administrators
- Describe how Active Directory achieves better scalability than previous versions of Windows NT
- Describe some of the key open standards that have been adopted in Windows 2000
- Describe some of the logical components that make up Active Directory

The release of Microsoft Windows 2000 gives us a lot to be excited about. Along with an operating system (OS) that is more stable, more scalable, and easier to maintain than previous operating systems, we have new features and possibilities that we have not seen before. Some of these new features are fairly minor (although none is insignificant). Others require you to change the way you think about your networks and the way you work with them in an enterprise.

In this chapter, we will start by giving you a brief overview of Windows 2000 and its features. We won't spend too long going through each feature in detail, because the focus of this book is Active Directory (which represents the most significant new element). However, knowing some of the new features and the way each one leverages Active Directory can help you see both the importance and significance of this new Microsoft technology.

Once we have finished with the new features, we will spend a little time going through the significant elements that represent Active Directory and allow it to work. This discussion is not intended to be exhaustive. Rather, it acts as an introduction to the topics that follow in this book.

Active Directory represents a monumental leap for Microsoft and its family of network operating systems (NOSs). Although some of the older concepts remain, their foundation is entirely different. This difference will affect the way you design and administer your networks, how you secure and delegate administrative tasks throughout your enterprise, and the troubleshooting techniques that you employ. This book will go into each of these details in turn, arming you with the knowledge you need to be effective with Windows 2000 and also to prepare for the 70-217 exam.

Windows 2000 Overview

Windows 2000 is the latest release from Microsoft. Previous versions of Microsoft NOSs were called Windows NT. **NT** is an acronym for **new technology**. For this new release, Microsoft has changed the naming scheme and has appended *Built with NT technology* to the CD. The name change might seem like a minor detail, but the marketplace has initially shown some confusion over what product Windows 2000 is intended to replace. Windows 2000 can replace earlier desktop OSs such as Windows 98—but it is important to note that the change is not minor. Windows 98 users who upgrade to Windows 2000 thinking that the change is on the same scale as a Windows 95 to Windows 98 upgrade will be in for quite a shock. This OS is radically different from an architectural point of view. The most natural succession is a move from Microsoft Windows NT Workstation 4 to Windows 2000 Professional.

It is true that any experience you have had with Microsoft Windows NT 4 will help you become familiar with Windows 2000. However, it is important that you do not overlook the changes that have occurred under the covers of this important OS. In the following sections, we will take a brief look at the additional features that have been integrated into Windows 2000.

The main focuses of Microsoft for this new version are:

- Increasing stability
- Increasing scalability
- Increasing security
- Reducing total cost of ownership (TCO)
- Supporting standards-based technologies

No single feature can achieve these goals. Microsoft has achieved these goals through a mix of features and new technologies. We'll outline each of them in a moment.

Before we go any further, we should take a look at the different flavors of Windows 2000 that are currently on the market. Four different versions of the OS are currently available, each with a designated purpose. Knowing what the versions are—and what issues they have been designed to address—will help you understand where Active Directory and its associated technologies fit in.

The Windows 2000 Family of Operating Systems

The previous version of Microsoft's NOS has three versions: NT Workstation, NT Server, and Enterprise Server. Each of these versions is intended to fit a niche within the enterprise. Windows 2000 has now added a fourth version to accommodate the new network functionality and performance that are demanded in enterprises today. The following list describes all four versions:

- *Windows 2000 Professional:* The replacement for Windows NT 4 Workstation. It incorporates many of the new Windows 2000 features and is fully compatible with Active Directory. In designing Windows 2000 Professional, Microsoft addressed issues such as stability, performance, and manageability. It addresses concerns with earlier Workstation products in the NT line by supporting a host of power management features in laptop and desktop computers. Windows 2000 Professional can also replace Windows 9.*x* on your users' desktops. Windows 9.*x* is a surprisingly lenient OS—it's seemingly able to run most anything thrown at it. This characteristic has been both a blessing and a curse. The OS works, so users want it; it is also difficult to manage and support, however. Windows 2000 Professional addresses this issue by increasing compatibility and offering extensive management capabilities. Windows 2000 Professional can operate as part of a network or as a standalone OS, making it suitable for all areas of your organization.
- *Windows 2000 Server:* A replacement for Windows NT 4 Server. The main difference between this product and Windows 2000 Advanced Server is scalability. Most of the other features are equal (with some notable exceptions). You can use Windows 2000 Server for file and print sharing. It also supports terminal services and applications. Its support for Internet Information Server 5 means that it can serve as a Web server on both the Internet and your intranet. It can also be useful in workgroups. Microsoft has been clear that this version of the OS is intended for small to medium-sized organizations. However, the company is not so clear on what this range constitutes. It is safe to assume that any place you currently have Microsoft Windows NT 4 is a good candidate for an upgrade to Windows 2000 Server.
- *Windows 2000 Advanced Server:* Like Windows 2000 Server, the advanced server product can operate as a file and print server, can host terminal services and applications, and can also operate as a Web server. In addition to these common features, Advanced Server also offers additional functionality in the areas of clustering, load balancing, and larger memory and CPU capacities. Because these advanced features are not important to the topics in this book, we will not cover them in detail.

- *Windows 2000 Datacenter Server:* The highest end of Microsoft's Windows 2000 family of OSs. It is designed with data warehousing in mind. That means even more memory capacity and more CPUs are supported. This product is intended for high-end, large-scale analysis projects. Its use and feature set are outside the scope of this book, and we will not be looking at this OS in detail.

As you can see, Microsoft has targeted all levels of enterprise with its new line of OSs. A full deployment of Windows 2000 will touch upon every level and desktop in your organization. To fully benefit from the new features offered by Windows 2000 and Active Directory, you will need to deploy Windows 2000 fully in your environment. Doing so means that every workstation and every server must be upgraded to the new OS. Let's take a look at some of the specific features that make a compelling argument as to why this comprehensive upgrade is a good idea.

The New Features in Windows 2000

What good would Windows 2000 be if nothing was new? No need to worry—Microsoft has added brand-new features that you have not seen before, and has also tweaked many of the older tools. In this section, we will take a brief look at some of these features. By becoming familiar with them, you will grow more acclimated to using the new OS.

The list of features shown in Table 1-1 is not (despite its length) exhaustive. Windows 2000 is packed with new features that may be significant from a development point of view but that do not have a huge impact on the work of system administrators.

Table 1-1 New features in Windows 2000

Feature	Description
Active Directory	Microsoft Windows NT 4 has been criticized because it does not scale well in an enterprise. Microsoft has addressed this criticism with Active Directory. Active Directory is the main focus of this book. Windows 2000 is fully integrated into Active Directory and was very much built with it in mind. It might surprise you to learn that Active Directory is not all Microsoft's idea. Indeed, it is largely built upon industry standards, which makes it both robust and compatible with other directories and systems. Active Directory addresses the scalability, security, and maintenance issues that will ensure a lower TCO. It also acts as a foundation for many Windows 2000 technologies such as Remote Installation Services, Group Policy, and Delegation of Authority.

Table 1-1 New features in Windows 2000 (continued)

Feature	Description
Active Directory Service Interface (ADSI)	Microsoft OSs have become known partly because of the familiar Graphical User Interface (GUI). Although this interface has been a useful tool for administrators, familiarity has bred contempt. Sometimes it just gets in the way. To address this situation, Microsoft has defined ADSI. ADSI is a set of Component Object Model (COM) components that open up Active Directory features to programmers. This feature is useful not only to development staff, but also to system administrators. ADSI is outside the scope of this book, but it is a safe bet that top-of-the-line Windows 2000 administrators will gain a familiarity with ADSI and what it can do.
Disk quota support	It has taken Microsoft a long time to recognize the need for disk quotas. However, they have finally arrived. Disk quotas allow you to designate a finite amount of space for a group or user on your Windows 2000 network. This assignment is done at the volume level on a server. The user can then be prevented from exceeding this limit. Disk quotas allow administrators to manage their disk resources and to ensure that no single user can monopolize a server.
Encrypted File System (EFS)	Windows 2000 supports the use of all the traditional methods of securing data, such as Access Control Lists (ACLs), user logon, and permissions. In addition, it supports EFS, which is a method to further encrypt data on an NTFS disk. EFS means that although hackers may be able to gain access to your system, they will not have access to the underlying data files. This is a useful feature for laptops or other computers that are often on the road (and therefore are more likely to be vulnerable to such attacks).
Group Policy	Group Policy is one of the key new features of Windows 2000. It allows you to both secure and maintain Windows 2000 Professional and Server computers in your enterprise. It leverages Active Directory for all of its features. Some of the key concepts of auditing and analyzing security rely upon Group Policy. Group Policy allows you to have a policy-based system that can be applied both at a high level and to many different systems at the same time. It is centrally managed and can be targeted at IP subnets, specific groups of computers or users, or an entire domain.
Internet Connection Sharing (ICS)	ICS allows you to refine the use of the Internet in small organizations or in the home office. Traditionally, home offices had a single point to the Internet: a dial-up connection. Each computer that required access to the Internet required its own dial-up connection. This setup was tedious and time consuming (not to mention rather expensive, because every system required its own modem). ICS allows you to make a single connection to the Internet and then share that connection among all the computers on your network. Although ICS would not work well for large organizations (which require a more robust system with better security options), for the home office this feature alone might be worth the price of admission.

Table 1-1 New features in Windows 2000 (continued)

Feature	Description
Internet Information Server (IIS)	This new version of IIS allows you to integrate your intranet site with the new multimedia features of Windows 2000 and Exchange 2000. It supports Active Server Pages (ASP) and document sharing across the Internet. In addition, it is now possible to limit the amount of processing time a Web site uses (**process throttling**); and IIS provides an extended reporting functionality that will help you identify which processes on the IIS system are using a disproportionate amount of CPU time.
Lightweight Directory Access Protocol (LDAP)	LDAP defines an industry standard method of accessing Active Directory data. By making Active Directory LDAP compliant, Microsoft has aided in the integration of Active Directory with other established systems. Microsoft has also enabled administrators who are already familiar with LDAP to get up to speed quickly on Active Directory integration.
Microsoft Management Console (MMC)	The MMC is the pervasive tool used to administer Windows 2000. The MMC is a flexible tool that can be customized to meet a specific customer's needs. It uses consoles to perform its tasks. You can create and combine consoles so they work the way you like. These custom consoles can then be distributed much the same as Microsoft Office documents.
Plug and Play	Most administrators are familiar with this functionality, which has been part of the Windows 9*.x* product for a long time. It has finally arrived in all its glory in Windows 2000. The idea behind Plug and Play is simple: Plug in a new piece of hardware (such as a network or video card), and Windows 2000 will detect its presence and load the necessary drivers without any interaction from the administrator. Plug and Play (in combination with the Hardware Compatibility List) should ensure that administrators no longer have to fight with complex configurations when adding new hardware to servers or Windows 2000 professional systems.
Remote Installation Services (RIS)	Microsoft has been supporting systems management for a long time, but one area has proven difficult to support: the initial installation of the operating system. RIS works by booting a computer from a Pre-Boot Execution Environment (PXE) read-only memory (ROM) chip. These chips are commonly found on network cards. Once the system has been booted, it is directed to an RIS server that contains images for installations of Windows 2000 professional. (Note that the current version of Windows 2000 does not support the installation of other OSs through RIS.) The image is then pulled down from the RIS server to the client. Because this is a scripted installation, no administrative interaction is required. Combined with ADSI, RIS is a powerful tool in your deployment arsenal.

Table 1-1 New features in Windows 2000 (continued)

Feature	Description
Windows Media Services	Windows 2000 now supports an extensive array of multimedia features, including streaming media and voice over IP. As bandwidth availability increases, video conferencing can finally become a reality. And because it is integrated into Windows 2000 and IIS 5, we can expect to see it adopted quickly.
Windows Scripting Host (WSH)	WSH is a powerful scripting language that can be used to configure systems or to apply changes to Windows 2000 systems on your network. Although it has been around for quite some time, the additional interfaces provided to Active Directory mean that its use has been extended dramatically. WSH is a host that can run scripts. It does not define the language that is being used for the scripts. As a result, you can write the scripts in whatever language you find most appropriate, including VBScript or JavaScript.

We will concentrate on some areas that are likely to have an impact on system administrators or deployment staff working with Windows 2000.

As you can see, this subset of new features opens up a whole new world for those just starting out using Windows 2000. Taken on their own, these features represent a wealth of new ideas for working—taken together, they represent a new way of looking at networking in your enterprise.

Windows 2000 Directory Services

This book concentrates on Active Directory, which is the directory service employed in Windows 2000. Although Active Directory is interesting within itself, you also need to understand how other Windows 2000 features leverage the functionality it provides to perform specific tasks.

Before we can get to these topics, let's look at a definition of what a directory service really is—and, more specifically, what Active Directory brings to the table. At the same time, we will explain the specific benefits, terminology, and introductory concepts that you will need to understand in order to be successful with Active Directory.

A **directory** is a collection of data that is related, in one way or another, to other pieces of data. In other words, a directory is a database. You probably use a directory in your everyday life without thinking too much about it. One of the most commonly used directories is the telephone directory, which keeps an alphabetized list of telephone subscribers.

A telephone directory is useful, but sometimes the data is not stored in a way that is useful for a particular function. For instance, if you want the telephone number of a Mr. Powell, it is an easy matter to look up his name in the P section. If you need a list of computer suppliers, however, things get more difficult. In order to use a simple telephone directory, you must know the names of the computer suppliers before you can look them up.

To solve this problem we have another directory, commonly known as the Yellow Pages. This directory also contains names and telephone numbers, but instead of being ordered by the names of subscribers, the list is sorted by category based around the jobs or tasks the subscribers perform. In this case, you could look up Computer Suppliers and then examine the list of names to find the one nearest you.

This directory is more useful; but it's a little inefficient, because it requires that you have two books on hand to find the information you commonly need. Sounds like a job for a computer, doesn't it? By keeping all this data in a database, you can easily sort or search on any criteria.

Telephone directories are a good way to present data on all subscribers to the telephone service. In fact, they are so useful that it did not take long for someone to realize that computer networks should be organized the same way. After all, if you think of your users and computers as subscribers to your network service, the analogy works quite well.

Networks have grown beyond the original vision of those who built the foundation of our industry. At the outset, no one could imagine that even single computers would want to talk to one another. Now, hundreds of thousands of computers need to share resources and to exchange data and processing cycles. Gaining control of these dispersed resources is not easy—but doing so is much simpler with a directory service in place.

So, a directory service is simply a central repository for data that describes the resources on your network. This data includes information about computers, users, user groups, printers, servers, and a whole host of other resources. A directory service both stores data and provides it to other systems. It allows various components on your network to identify themselves and to interact. In Windows 2000, this fundamental concept powers many of the new features.

In the past, things were very different. On early networks, each computer had its own directory service (a list of user accounts). They stored far less data than today's systems, because there wasn't as much to know. From these individual directory services, networks shifted to central repositories stored on server machines. Each of the servers in an organization had its own directory. So, if a user needed access to two servers, a user account (or, in Windows 2000 terms, a **user object**) had to be created on both machines, quite independent of each other.

Microsoft Windows NT 4 employs a different method. In this case, it uses a directory service based around the domain model. All data about objects within the domain is stored in a single database. One server in the organization has a special task—that task is to accept changes to the directory, and then to distribute those changes to other machines in the domain so they can service directory requests (such as validation for logon purposes).

As we move into the twenty-first century, computer networks have grown exponentially. The older model used in Microsoft Windows NT 4 has proven successful, but it is unlikely to survive the move to global networking that is currently under way. It is time for something different—an evolution of directory services. It is time for Active Directory.

Windows 2000 and Active Directory

Active Directory is the name given to the directory service employed in Windows 2000. Naming aside, the goal of Active Directory is as we just outlined. Active Directory is a central source of data about resources on a Windows 2000 network. It is both a repository (or storage area) and a service that can provide data to applications and features outside of Active Directory. This dual purpose is illustrated in Figure 1-1.

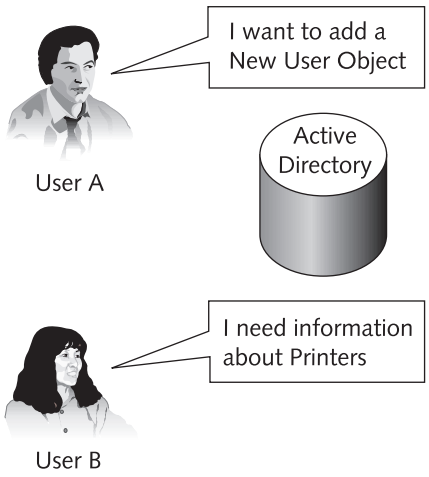

Figure 1-1 The dual nature of Active Directory

When reading about Active Directory and Windows 2000, you will often see general terms thrown about. You might wonder how Active Directory specifically addresses them. Let's take a brief look at some of the terms used and see how Active Directory works to help in these areas.

We will examine the following areas:

- Ease of administration
- Scalability
- Standards support

By understanding the fundamental ways in which Windows 2000 and Active Directory address these issues, you can better understand the significance of what you read in this book.

Ease of Administration

Microsoft Windows NT 4 goes a long way toward simplifying administrative tasks. As we described earlier in this chapter, there was a time when each server on a network operated as though it existed in its own little world. The concept of **domains**, introduced in Windows NT, simplifies this concept by having a single point of authentication for everyone.

The concept of domains has been retained for Windows 2000. As a result, the skills you have developed in designing and implementing domains are still valuable. However, there are some subtle differences in Windows 2000. For instance, for a user to access data in another Windows NT domain, an administrator must create what is known as a **trust**. A trust basically means that users and groups in one domain are trusted to access data or resources in another domain. This system works well, but in multinational organizations, it can result in a complex web of trusts. By default in Windows 2000, these domain trusts are created automatically. What's more, they are **transitive**, which means that if domain A trusts domain B, and domain B trusts domain C, then A in effect trusts C. This feature very much simplifies administration and the assignment of access to resources in an enterprise.

Scalability

One of the problems that became apparent in Windows NT 4 is the limited size of the security database. At the time NT 4 was introduced, a 40MB database seemed huge; as networks have grown, however, it has become clear that this arbitrary size is a factor in limiting potential growth.

Fortunately, Microsoft has addressed this issue by effectively removing limits from the size of the Active Directory database. Of course, there is a physical limit; because it can be defined as more than 16 million different objects, however, it is unlikely that we will run out of room any time soon.

Another scalability issue came about when widely dispersed organizations began to implement Windows NT 4. In this earlier iteration of Microsoft's NOS, one server acts as the keeper of the data. It is unique in that it is the single place on the network that accepts changes to the data. This server is known as the Primary Domain Controller (PDC). All other domain controllers exist only to service local requests for directory data. These servers are known as Backup Domain Controllers (BDC) because they back up the functionality of the PDC.

This system works well, except that the position of the PDC in an infrastructure can affect the amount of traffic moved across the network cable. What's more, a single point of failure exists, because if the PDC goes down for some reason, things can get pretty hairy. It's possible to promote a BDC and make it the new PDC, but that BDC is unlikely to be in an optimal location. To solve this problem, Microsoft has made all domain controllers in a Windows 2000 domain equal. They all act as though they are PDCs. Now a new problem has been introduced: If any domain controller can accept changes to the directory, how are all copies of the directory updated with the changes? The answer is Active Directory replication, which we will cover in detail in Chapter 14.

Open Standards Support

Microsoft has introduced support for Internet standards into its core OSs, which should lead to earlier adoption and even better scalability over time. An example of

open standards support is the adoption of Domain Name System (DNS) as the underlying naming format for domains. In fact, DNS is so fully integrated into Windows 2000 that you simply cannot install Active Directory without it.

Active Directory can share its data through LDAP, which we described earlier. The LDAP standard was designed to overcome some of the overhead associated with the original Directory Access Protocol. LDAP is not the only protocol that can be used to gather data from Active Directory—Microsoft also supports Hypertext Transfer Protocol (HTTP). Because HTTP is supported in all Web browsers, you can see that the door is wide open for tools that can utilize the directory information.

Windows 2000 has taken a big step to being more open and scalable by using these proven industry standards. By removing the OS's reliance on more proprietary protocols, such as NetBIOS, Microsoft has ensured that Windows 2000 will work efficiently and be more integrated with other networks, such as Novell NDS and the Internet than ever before.

The Physical and Logical Structure of Active Directory

We will take a closer look at the elements that make up Active Directory in Chapter 2. Before you start on your journey, however, let's briefly describe some of the terms you will see, and let's explain conceptually how Active Directory works.

Active Directory is a database, pure and simple. Databases are stored in rows and columns, and Active Directory is no different. In fact, Active Directory is a single (albeit very large) table. This table resides in a single file that is essentially copied to all domain controllers. Once the database is copied, only changes are sent from domain controller to domain controller (this is a process known as **replication**).

Each row of data in the Active Directory database describes a resource on the network. In Active Directory terms, the many different types of resources are known as **objects**. Objects have properties, which are defined by each column in a row; they are also called **attributes**. Anyone familiar with a database application such as Microsoft Access or Microsoft SQL Server should be familiar with the concepts detailed here. This structure is illustrated in Figure 1-2.

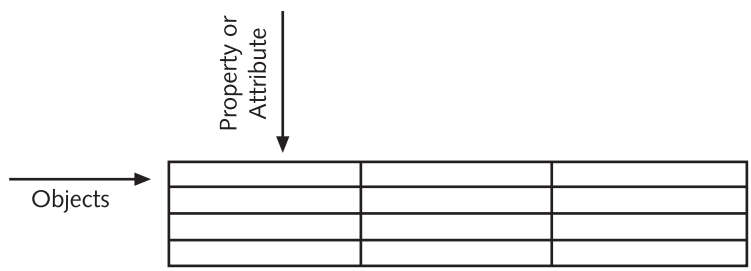

Figure 1-2 A view of Active Directory as a database table

Of course, Active Directory cannot accept just any kind of object. In fact, each object type has to be defined before it can be used. The **Active Directory Schema** defines which objects can be stored within Active Directory and which properties or attributes they can have. This schema is very flexible. Although it is not possible to completely remove the various object types that Microsoft has defined for you, it is entirely possible to define new object types. These object types are then replicated along with all other Active Directory data in the replication process.

You might also see the term **metadata** in your travels around the world of Windows 2000. In fact, in the terminology we're using here, each attribute is considered to be Active Directory metadata. Metadata is data about data. In this case, it means that the properties of an object in Active Directory describe something about that object.

Although it is convenient to alter the Active Directory Schema and add object types and attributes that you want, you should also exercise caution. Definitions can be added to Active Directory, but they can never truly be deleted—instead, they can be **deactivated**, which means they are not used but still exist within the directory data.

The Active Directory Schema is a second table that exists on every domain controller. Once again, it is a simple table of rows and columns, just like a Microsoft Excel spreadsheet or simple database file. This concept might confuse you, because all representations of Active Directory show this simple table in a hierarchical fashion. That's the case because part of the Windows 2000 OS takes what is essentially a two-dimensional representation of the data and gives it to you in the form you require.

Logical Components

How is Active Directory data organized? It is all well and good to be told that a database contains all the data about each object in your organization, but how does that help you, the system administrator, do your job?

We can answer this question by taking a look at a logical view of a Windows 2000 network. A **logical view** means that you are looking at representations, or interpretations, of the underlying data. The data itself is not changed—it is simply your view of the data that is changed.

In the following paragraphs we will give you brief descriptions of the following:

- Domains
- Groups
- Organizational Units

These descriptions are not intended to be exhaustive. However, by becoming acquainted with the concepts now, along with how they fit in with the older style Microsoft Windows NT 4 concepts, you will be well placed to move ahead to more advanced definitions and other new features of Windows 2000.

The first logical structure will be familiar to you: the *domain*. Domains really have not changed very much from previous versions of Microsoft Windows NT 4. A domain operates as a single entity and boundary for security purposes. Domain administrators have ultimate power over the domain; they can create new user accounts, printers, and groups.

Of course, Windows 2000 is bigger than a single domain—it is now an enterprise-level directory service. Although in previous versions the domain administrator could be thought of as the ultimate authority, this is no longer the case. The ultimate authority in a Windows 2000 network is an enterprise administrator, because he or she has exclusive rights over Active Directory and permissions in all domains.

You will often see Active Directory described as both a Directory, and as a Directory Service. The context dictates the usage of these terms. When we talk about a Directory Service, we are actually talking about two different things—the storing of the data (in the Directory) and the ability to supply that data to applications (offering a Service.)

Microsoft Windows NT 4 has the concept of **groups**, and this concept has been extended into Windows 2000 with a couple of new twists. The first twist is that a fully deployed implemented Active Directory includes a new type of group: the Universal group. It is used to assign permissions throughout an enterprise. The second twist is the addition of another level of organization: an Organizational Unit (OU).

You cannot assign access permissions to members of an OU simply through their membership, because OUs don't have security tokens. However, OUs serve as a way to organize resources and to apply Group Policy to them. Group Policy is covered in detail in Chapter 10; it forms a foundation for much of what you will do on your network.

As you can see, these basic concepts are based on what you are used to, with some new twists and turns that give you more flexibility and control. Many more new terms and definitions will be necessary for you to get a good understanding of Active Directory. These, along with a more detailed discussion of the elements covered in this chapter, will be presented in Chapter 2.

Working with Active Directory in Your Enterprise

Having a new directory service in place is one thing, but what exactly does it do for you? It is useful to know how to define Active Directory and to see some of the ways it can help you maintain and administer your network—but you may wonder what other day-to-day tasks will be affected by enabling Active Directory on your network.

That is the topic of the rest of this book, and it could ultimately lead to your acceptance and use of Active Directory. Active Directory can help you directly with many tasks or problems, and in other, more subtle ways, it can aid you in getting your job done. This section will briefly outline the ways Windows 2000 and this book can help you. Each option

will be illustrated in far greater detail in later chapters. This section simply aims to define highlights of both Windows 2000 and the new features you will want to implement.

Working with DNS

One of the first things you will need to consider is the impact of the adoption of the aforementioned standards. Microsoft Windows NT 4 relied heavily upon NetBIOS for both name resolution and naming standards. Windows 2000 has now moved toward using the industry standards of DNS. What's more, an increasing number of organizations have moved some of the name resolution work to the Internet.

The Internet also uses DNS as its name-resolution scheme. As a result, you will have to be careful how you name your Windows 2000 domains. It's important to be aware of the possible consequences of naming your domains in such a way that they conflict with someone who already has an Internet presence.

You may deliberately decide to share an Internet name, or you may have an Internet presence and want to keep Windows 2000 as a separate entity (by choosing a different name). Whichever route you choose, careful planning will be key to your success. Don't forget, Internet names are regulated and must be registered. If your Windows 2000 network will be connected to the Internet, you cannot use a domain name that already exists or that has already been registered.

DNS is a complex system—it is at the very heart of the Internet, and it alone allows you to find all the Web sites you are familiar with. There has never been a better time to get acquainted with the details of DNS than now. Windows 2000 does not function without it, and you will not be able to implement Active Directory without a good understanding of all its components. Your clients will perform name resolution all the time—they will be searching for network services and resources, and this process is taken care of by DNS. You will have to scale DNS servers in your enterprise and be aware of methods you can use to place DNS servers in remote locations to handle the load and avoid slow network bandwidths.

The Installation Process

Given the nature of Active Directory, it is not likely that you will be lucky enough to simply install it throughout your enterprise in one swoop. Not only would it be complex to do so, but you probably already have a network infrastructure in place.

Moving from a Microsoft Windows NT 4 system to a Windows 2000 system is not too complicated. However, adding Active Directory involves more than simply installing the core OS. In fact, as you will see in Chapter 5, there is no way to install Active Directory along with the core OS. The step to install Active Directory is performed afterward. This flexibility allows you both to promote systems to operate as domain controllers in your organization, and also to demote them back to plain old servers (something sorely missing in previous Windows NT versions).

It should also be noted that not all Active Directory installations are created equally. When you're moving an older domain into the new style with Active Directory, you have two different levels of functionality, also known as **modes**. The first is known as **mixed mode**; essentially, it means you have older OSs operating on your new Windows 2000 network. Once you have fully upgraded, you can move to **native mode**. You should know about some significant differences as you move from one mode to the other; these will be covered in Chapter 5.

New Overhead

The additional functionality of a Windows 2000 implementation with Active Directory does not come without some overhead. Most of that overhead is in the increased knowledge you must have on the inner workings of Active Directory. For instance, in previous versions, you really don't care much about how data is copied from the PDC to the BDC. The process is largely automatic, with few configurable options. In Windows 2000, this process has changed. You will need to gather data on your TCP/IP network and get accurate data on the amount of network bandwidth available to you. Designing a Windows 2000 network suddenly became more complex—but, fortunately, the rewards are greater.

Delegating Tasks

Of course, where would we be without our user community? Once you have Windows in place and working, you will find that most of the everyday tasks are much the same as you have experienced previously: They include adding users, creating groups, and assigning permissions to network resources. We will take a look at these processes in detail later. With the new delegation-of-authority options, however, you will be able to assign people permission to perform some of the most common functions. We'll show you how to do this in Chapter 7 and tell you why it is a good idea to take advantage of this feature (believe me, you'll be busy enough).

Active Directory Maintenance

It should come as no surprise to find that Active Directory itself will need some maintaining. We're not talking about the users and groups—we mean the underlying files that allow it to work. Because Active Directory is a database, that database must be backed up and restored in the event of failure. Because every domain controller is a peer, a lot can change between the time a domain controller goes offline and the time it is once again made functional. You must be aware of how Active Directory deals with such circumstances, and how you can both maintain and optimize Active Directory in your environment.

Group Policy

We have not spoken much about Group Policy in this chapter. This is not because it isn't going to be significant in your enterprise—actually, quite the opposite is true. Group Policy is a huge part of what will make Windows 2000 a significant upgrade for your organization. It is so important that this book includes no fewer than three chapters (Chapters 10, 11, and 12) that discuss both the core functionality of this feature as well as two specific areas in which it can be of help.

Group Policy builds upon the functionality of Active Directory to make Windows 2000 a more controlled and manageable environment. It enables much of the TCO savings that we talked about earlier. These features include setting security at clients and servers along with software distribution. Group Policy uses the Active Directory database along with the logical elements of a Windows 2000 network as outlined earlier. This fact should help reinforce in your mind just how important the planning aspects of your Windows 2000 rollout will be. Without a solid foundation, you cannot successfully implement these features.

Replication and Security Templates

You should also know about two other areas of interest. The first is the method Active Directory uses to replicate all this enterprise data from one point to another. Microsoft has the responsibility not only of making sure that all changes are available at all times, no matter where you are on the network, but also of ensuring that the replication of this data does not overwhelm slow links or the servers themselves. We will walk you through the replication process in some detail in Chapter 14. Once you have an understanding of how it works, you should be able to follow replication throughout your organization and design an infrastructure that can support the amount of data that must be replicated.

Finally, you must know how to secure your network through security templates and Group Policy. **Security templates**, discussed in Chapter 15, are merely predefined groupings of settings that can be applied to all machines that are grouped in a logical way (through domains or OUs, for instance). By applying security policies this way, you can ensure that they are applied consistently and that all Windows 2000 systems are treated equally.

Chapter Summary

- In this chapter, we looked at some of the new features offered in Windows 2000. We also introduced some of the concepts that will be discussed in the rest of this book. We began by examining Microsoft's main Windows 2000 design goals. Microsoft has stated that its goals are increased stability, scalability, security, reduced TCO, and adherence to industry standards.
- We also defined the different versions of Windows 2000 that are currently available, describing how each compares to previous versions of Microsoft Windows NT 4

and providing information to help you decide which version is right for your organization. We saw that four versions currently exist: Windows 2000 Professional, Windows 2000 Server, Windows 2000 Advanced Server, and Windows 2000 Datacenter Server.

- Windows 2000 Professional is the heir to the Microsoft Windows NT 4 Professional throne. It can also replace Windows 9.*x* in corporate environments. Windows 2000 Server replaces Microsoft Windows NT 4 Server and can act as a file and print server for small to medium-sized organizations. Windows 2000 Advanced Server includes additional functionality, such as clustering and load balancing. It is intended for large organizations. Datacenter Server is intended for large database applications, such as data warehousing. Microsoft has added scalability functionality to the Advanced Server and Datacenter Server products, including support for more RAM and CPUs.
- We then looked at some of the new features introduced in Windows 2000. The list was not intended to be complete—rather, it attempted to show some of the ways in which Windows 2000 can improve the workload of a system administrator. These features include Active Directory, disk quotas, EFS, and Group Policy. They combine to make Windows 2000 far more useful than older versions of Windows NT in your enterprise.
- We then defined the term **directory services**. We explained that a directory service—and therefore the Active Directory component of Windows 2000—is simply a database containing information about the resources available in your enterprise. You learned that similar to a telephone directory, every user, computer, and group (among other things) has an entry in the Active Directory database. We explained that these different types of information are known as **objects**.
- Each object in Active Directory has **attributes**. You can query Active Directory for these attributes using the administrative tools in Windows 2000 or by using LDAP or ADSI and the WSH. You learned that a common term used to describe these attributes is **metadata**; metadata is data about data.
- We briefly looked at the older-style directory service that shipped with Microsoft Windows NT 4, and how it fails to scale to today's multinational organizations. You learned that the old-style PDC and BDC arrangement has been replaced with a new type of domain controller. All domain controllers in a Windows 2000 network operate as though they were PDCs, which helps increase the scalability of Windows 2000.
- We saw that some of the most common administrative tasks, such as creating trust relationships across domains, have been virtually eliminated in Windows 2000. Trusts are automatically configured as domains are created.
- We then examined some of the physical and logical objects that help a Windows 2000 network function. These objects include domains, objects, attributes, groups, and OUs. These objects allow the administrator to better define and assign permissions throughout the enterprise.

- We next explored several topics that will be covered in more detail as you work your way through this book. These topics include DNS, installing Windows 2000 domain controllers, and the different modes (**mixed mode** and **native mode**) in which Windows 2000 must operate when older-style OSs participate on the network.
- We introduced the concept of Group Policy and why it will be a large part of your enterprise. We discussed several areas where it will be important, including the assignment of security settings along with software deployment.
- Finally, we took a brief look at some security issues and how they might be solved. We defined security templates in order to prepare you for later chapters of this book.
- This chapter set out to introduce you to some new terms and to prepare you for what is to come. We laid the groundwork for a good understanding of both Windows 2000 and Active Directory. We also introduced key features and functionality.